Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of Advanced Methods to Target and Eliminate Unlawful Robocalls Call Authentication Trust Anchor	CG Docket No. 17-59 WC Docket No. 17-97

REPLY COMMENTS OF NEUSTAR, INC.

Neustar, Inc. ("Neustar") hereby submits the following reply comments in response to the Federal Communication Commission's ("Commission" or "FCC") *Further Notice*[1] and the comments of other parties regarding methods to target and eliminate unlawful robocalling.

I. INTRODUCTION

Neustar has a long history with telephone number administration, Caller ID and the STIR/SHAKEN protocols used for Caller ID authentication. Neustar is the nation's largest provider of Caller Name ("CNAM") information to service providers for Caller ID displays. As such, Neustar has a strong interest in protecting the authenticity of Caller ID information and preserving consumer's trust in telephone communications. To that end, Neustar is a pioneer in call authentication as a co-author of STIR standards, active contributor to the SHAKEN

[1] *See Advanced Methods to Target and Eliminate Unlawful Robocalls*, Report and Order and Further Notice of Proposed Rulemaking, CG Docket No. 17-59, FCC 17-151 (rel. Nov. 17, 2017); *Advanced Methods to Target and Eliminate Unlawful Robocalls*, Declaratory Ruling and Third Further Notice of Proposed Rulemaking, CG Docket No. 17-59, WC Docket No. 17-97 (rel. June 7, 2019) ("*Declaratory Ruling" and "Further Notice*" respectively).

framework and the exclusive operator of the Alliance for Telecommunications Industry Standards ("ATIS") Robocalling Testbed, where real-world STIR/SHAKEN implementations are tested for interoperability with Neustar's reference implementation.[2]

Due to its involvement with CNAM, Neustar works with legitimate enterprises to help them deliver a robust Caller ID experience to their customers, particularly those with mobile phones. Instead of simply delivering the traditional fifteen character Caller Name display, Neustar enables enterprises to deliver logos and other information to assist call recipients in determining whether to trust an incoming call. In addition, to prevent the blocking of legitimate calls, Neustar works with well-vetted legitimate enterprises to help register their telephone numbers with robocalling analytics companies.

Neustar has long been supportive of the Commission's efforts to combat illegal robocalling. With the exception of calls appearing to originate from the categories of telephone numbers described in the Commission's 2017 *Call Blocking Order*[3] – invalid, unallocated, unallocated, or do-not-originate – which Neustar agrees can only be illegal and should be unilaterally blocked by providers, Neustar believes that consumers should be empowered as much as possible with regard to the calls that they receive. So that consumers can make more informed decisions about incoming calls is one of the reasons that Neustar works with legitimate enterprises to help them provide more robust Caller ID information to call recipients.. In that same vein, Neustar supports the action taken by the Commission in the *Declaratory Ruling* that allows providers to use analytics to block suspected illegal robocalls, with consumers having the ability to opt-out of such blocking. Because of the opportunity to opt-out, the consumers remain

---

[2] *See*, https://www.home.neustar/atis-testbed/index.php (last visited August 22, 2019).

[3] *Advanced Methods to Target and Eliminate Unlawful Robocalls*, Report and Order and Further Notice of Proposed Rulemaking, 32 FCC Rcd 9706, 9727 (2018) (*Call Blocking Order*).

in control of their communications choices. Consumers can decide whether to allow providers to block at the network level or to make their own decisions on a call by call basis.

In the *Further Notice*, the Commission raised several issues concerning its proposal to create safe harbors for service providers that block suspected illegal robocalls based on the STIR/SHAKEN Caller ID authentication. In these reply comments, Neustar addresses several of these issues and responds to certain comments of other parties.

II. THE COMMISSION SHOULD ADOPT A BROAD SAFE HARBOR FOR PROVIDERS THAT BLOCK CALLS BASED ON ANALYTICS THAT INCORPORATE STIR/SHAKEN AUTHENTICATION

In the *Further Notice*, the Commission proposed a narrow safe harbor limited to providers that block calls that fail the STIR/SHAKEN authentication.[4] As proposed, such a safe harbor would be applied only to the blocking of calls that fail STIR/SHAKEN but would not apply, for example, to call blocking programs that consider the level of attestation a call receives. Neustar agrees with parties that suggest that the Commission adopt a broader safe harbor.[5]

In Neustar's view, STIR/SHAKEN alone is not sufficient to determine whether a call is an illegal robocall that should be blocked or is a legitimate call that should be completed. Rather than using STIR/SHAKEN as a standalone determinant for illegal robocall blocking, providers will obtain better results if they include STIR/SHAKEN in the analytics that they deploy to combat illegal robocalls.[6]

In the *Declaratory Ruling*, the Commission authorized providers to block suspected illegal robocalls using their own analytics. Rather than the narrow safe harbor proposed in the

---

4 *Further Notice* at 49.

5 *See, e.g.*, AT&T Comments at 11, Verizon Comments at 11, T-Mobile Comments at 6

6 See, T-Mobile Comments at 8, First Orion Comments at 9, TNS Comments at 3, and USTelecom Comments at 2.

Further Notice, Neustar recommends that the Commission apply the safe harbor to providers that incorporate STIR/SHAKEN into the analytics that they are using to block suspected illegal robocalls. This broader safe harbor for incorporating STIR/SHAKEN would not be limited just to blocking calls that fail STIR/SHAKEN but also, for example, to possibly blocking calls based on the level of attestation. This offers a safe harbor to a provider that blocks a call with a high STIR/SHAKEN attestation if other analytics give the provider a reasonable belief that the call is likely an illegal robocall; conversely, a call that has low attestation may be allowed to be completed if other analytics indicate the call is likely valid. A broad safe harbor will also incent providers of all sizes to implement STIR/SHAKEN more rapidly in order to obtain the safe harbor.[7]

An additional benefit of a broad safe harbor when STIR/SHAKEN is included as part of the analytics used by providers to block illegal robocallers is that, per the construct established by the Commission in the *Declaratory Ruling*, consumers will have the opportunity to opt-out of the call blocking, including call blocking based on STIR/SHAKEN. While many consumers are desperate to reduce the robocalls that they receive and will likely not opt-out of robocall blocking analytics that includes STIR/SHAKEN verification, others may opt-out of this call blocking until the rough edges of STIR/SHAKEN are smoothed out.

III. CALLERS MUST RECEIVE NOTIFICATION WHEN THEIR CALLS ARE BLOCKED TO ENABLE UNBLOCKING OF WANTED CALLS

The *Further Notice* asks whether the Commission should require voice service providers to provide a mechanism for identifying and remedying the blocking of wanted calls, possibly by sending an intercept message or other indication that the call has been blocked.[8] If calls are

---

7 *See Further Notice* at ¶62. See, also, AT&T Comments at 11.

8 *Further Notice* at ¶58.

being blocked, callers must be informed so that legitimate callers can contact service providers to prevent future blocking. Further, if wanted calls containing an urgent message are blocked, a return signal in some fashion will alert the caller that an alternate means of communication should be attempted. Neustar already works as an intermediary between legitimate enterprises and service providers and their analytics companies to help vetted enterprises get their numbers registered. To date, Neustar has registered over seventy companies and hundreds of thousands of numbers of legitimate enterprises with the analytics companies that the leading mobile operators utilize. This Neustar solution helps to prevent the blocking of legitimate calls, and if calls are being blocked, provides callers a way to seek remedy across all of the mobile operators.[9]

IV. MAJOR PROVIDERS SHOULD BE ABLE TO IMPLEMENT STIR/SHAKEN BY THE END OF 2019

The *Further Notice* asks whether the Commission should mandate that major service providers implement STIR/SHAKEN if they have not done so by the end of 2019.[10] Neustar supports broad adoption of STIR/SHAKEN as rapidly as possible. Based on Neustar's experience as the operator of the ATIS Robocalling Testbed, we believe that the major service providers should not have difficulty in meeting the end of 2019 deadline for initial, voluntary implementation of STIR/SHAKEN, as at least half of them have already completed testing.

V. SIGNIFICANT STIR/SHAKEN IMPLEMENTATION ISSUES REMAIN

Although Neustar supports a broad safe harbor for service providers that use STIR/SHAKEN verification and robocalling analytics to block calls for which they have a reasonable belief are illegal robocalls, there are still a number implementation issues that cause

---

9 *See,* ACA International Comments at 10, PACE Comments at 4.

10 *Further Notice at ¶71.*

concern. For example, Neustar agrees with INCOMPAS that attestation must be addressed.[11] As INCOMPAS points out, under current STIR/SHAKEN procedures, service providers that resell service on telephone numbers of others carriers are not able to sign for the calls made by their customers, many of which are enterprises utilizing multiple competitive carriers for least cost routing. As a result, the calls made through competitive providers by these enterprises are likely to have a lower level of STIR/SHAKEN attestation. The proper solution to this is for some form of delegation that allows vetted non-carrier entities to sign calls with the same high level attestation as carriers that obtain direct North American Numbering Plan resources. If the industry does not deal with this issue appropriately, the Commission may need to step in to make sure competitive providers and certain enterprises are not harmed.

Additionally, legacy networks create challenges for implementation of STIR/SHAKEN, which currently requires Internet Protocol. Recognizing this near-term limitation of in-band STIR/SHAKEN, Neustar continues to support the implementation of complementary call authentication technologies, such as out-of-band authentication that can be integrated into the STIR/SHAKEN authentication framework.

VI. A BROAD SAFE HARBOR FOR BLOCKING CALLS BASED ON STIR/SHAKEN ANALYTICS MAY ENCOURAGE LEGITIMATE OVERSEAS PROVIDERS TO IMPLEMENT STIR/SHAKEN

Legitimate foreign providers will be incented to implement STIR/SHAKEN for their traffic bound for the United States if the Commission provides the broader safe harbor for service providers in the United States to block suspected illegal robocalls based on STIR/SHAKEN verification and analytics. If an overseas provider does not implement STIR/SHAKEN, calls from its customers to the United States will go through gateways that will

[11] *See*, INCOMPAS comments at 6, Telnyx Comments at 1.

provide the lowest level of standardized STIR/SHAKEN attestation. If U.S. providers are permitted to block calls using STIR/SHAKEN verification and analytics, calls with a low level of attestation risk being blocked as potential illegal robocalls. To ensure that their customers' calls to the United States are not blocked, international providers will be incented to implement STIR/SHAKEN for U.S bound traffic. These providers can then attest for their own calls, which will reduce the risk of attestation-based blocking.

August 23, 2019

Respectfully submitted,

/s/ Kevin A. Hughes

_____

Kevin A. Hughes
Exec. Vice President and General Counsel
NEUSTAR, INC.
21575 Ridgetop Circle
Sterling, VA 20166